MATHEMATICAL TRIPOS PART III (2005–06)

Elliptic Curves - Problem Sheet 2 of 4 **T.A. Fisher**

16) Let $C \subset \mathbb{P}^2$ be a smooth cubic defined over a field K. Show that if $\mathrm{char}(K) \neq 3$ then C has exactly 9 points of inflection (over $\overline{K}$).

17) Let $a, b \in K$ with $2b(a^2 - 4b) \neq 0$. Let E and E' be the elliptic curves

$$E : y^2 = x^3 + ax^2 + bx, \qquad E' : y^2 = x^3 - 2ax^2 + (a^2 - 4b)x.$$

In lectures we defined an isogeny $\phi : E \to E'$ of degree 2. Find an isogeny $\psi : E' \to E$, also of degree 2. Can you describe the composite $\psi \circ \phi$ in $\mathrm{End}(E)$?

18) Let A be an abelian group. Let $q : A \to \mathbb{Z}$ be a map satisfying

$$q(x + y) + q(x - y) = 2q(x) + 2q(y)$$

for all $x, y \in A$. Show that q is a quadratic form.

19) Find a translation-invariant differential ω on $\mathbb{G}_m$. If $\phi, \psi : \mathbb{G}_m \to \mathbb{G}_m$ are morphisms of group varieties, show that $(\phi + \psi)^*\omega = \phi^*\omega + \psi^*\omega$.

20) Let E be an elliptic curve over $\mathbb{F}_{13}$ with $E(\mathbb{F}_{13}) \cong \mathbb{Z}/9\mathbb{Z}$. Find the order of $E(\mathbb{F}_{13^2})$ and determine whether this group is cyclic.

21) Let E_1 and E_2 be elliptic curves over $\mathbb{F}_q$. Show that if there is an isogeny $\phi : E_1 \to E_2$ defined over $\mathbb{F}_q$ then $|E_1(\mathbb{F}_q)| = |E_2(\mathbb{F}_q)|$.

22) Let p be a prime. Let E be an elliptic curve over $\mathbb{F}_p$ with $|E(\mathbb{F}_p)| = 1 - a + p$. Let $\phi : E \to E$ be the p-power Frobenius, and put $\widehat{\phi} = a - \phi$ in $\mathrm{End}(E)$. Show that
(i) $\deg(n + \phi) = \deg(n + \widehat{\phi}) = n^2 + an + p$ for all $n \in \mathbb{Z}$.
(ii) $\deg(m + \phi\,\widehat{\phi}) = m^2 + 2pm + p^2$ for all $m \in \mathbb{Z}$.
(iii) $\phi\,\widehat{\phi} = \widehat{\phi}\,\phi = [p]$.
(iv) E is supersingular (i.e. $E(\overline{\mathbb{F}}_p)[p] = 0$) if and only if $p \mid a$. (You may quote that if $\alpha : E \to E'$ is an isogeny then $|\ker(\alpha)| = \deg(\alpha)$ if and only if α is separable.)
[Hint for (ii): It is enough to prove this for three distinct values of m. Why?]

23) Let R be a commutative ring of characteristic 2, which contains a non-zero element a with $a^2 = 0$. Show that $F(X, Y) = X + Y + aX^2Y$ is a non-commutative formal group over R.

24) Let $F(X, Y)$ be the formal group attached to an elliptic curve with Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

Show that

$$F(X, Y) = X + Y - a_1XY - a_2(X^2Y + XY^2) + (a_1a_2 - 3a_3)X^2Y^2 - 2a_3(X^3Y + XY^3) + \ldots$$

25) Show that if $F(X, Y)$ is a formal group over R then there exists a unique power series $i(T)$ in $R[[T]]$ with $F(T, i(T)) = 0$. Find $i(T)$ for the multiplicative formal group $\widehat{\mathbb{G}}_m$.

26) Let R be a ring of characteristic zero, and let $K = R \otimes \mathbb{Q}$. Suppose that $f(T) = \sum_{n=1}^{\infty}(a_n/n!)T^n$ and $g(T) = \sum_{n=1}^{\infty}(b_n/n!)T^n$ are power series in $K[[T]]$ satisfying $f(g(T)) = g(f(T)) = T$. Show that if $a_1 \in R^*$ and $a_n \in R$ for all n, then $b_n \in R$ for all n. [Hint: Repeatedly differentiate $f(g(T)) = T$ and put $T = 0$.]

27) For A an abelian group and $n \geq 2$ an integer we define

$$q(A) = \frac{\#\mathrm{coker}([n] : A \to A)}{\#\ker([n] : A \to A)}.$$

(It is undefined if either group is infinite.) Show that if $A \subset B$ is a subgroup of finite index, and either $q(A)$ or $q(B)$ is defined, then they are both defined and $q(A) = q(B)$.

28) Let K be a local field, i.e. K is a field of characteristic zero, complete with respect to a discrete valuation and with finite residue field. Let E/K be an elliptic curve and $n \geq 2$ an integer. Show that
(i) $[\mathcal{O}_K^* : (\mathcal{O}_K^*)^n] = |\mu_n(K)|[\mathcal{O}_K : n\mathcal{O}_K]$,
(ii) $[E(K) : nE(K)] = |E(K)[n]|[\mathcal{O}_K : n\mathcal{O}_K]$.
Find the order of $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$ for all primes p.

29) Let E be an elliptic curve, and let $\mathrm{Isom}(E)$ be the set of all maps $E \to E$ that are isomorphisms of curves. It is a group under composition. Show that the translation maps form a normal subgroup.

30) Let C be the plane cubic $aX^3 + bY^3 + cZ^3 = 0$ with $a, b, c \in \mathbb{Q}^*$. Show that the image of the morphism $C \to \mathbb{P}^3$; $(X : Y : Z) \mapsto (X^3 : Y^3 : Z^3 : XYZ)$ is an elliptic curve E, and put E in Weierstrass form.